
The Vulnerability Analysis Project (VAP)

William J. Orvis

DOE Computer Security Conference

Seattle, April 22-26, 1996

UCRL-MI-123880

**Work performed under the auspices of the U.S. Department of Energy by
Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.**

What is VAP?

Vulnerabilities in modern computer systems and networks make it possible for unauthorized people to subvert security for malicious purposes. Systems today have many such vulnerabilities, with more being discovered daily.

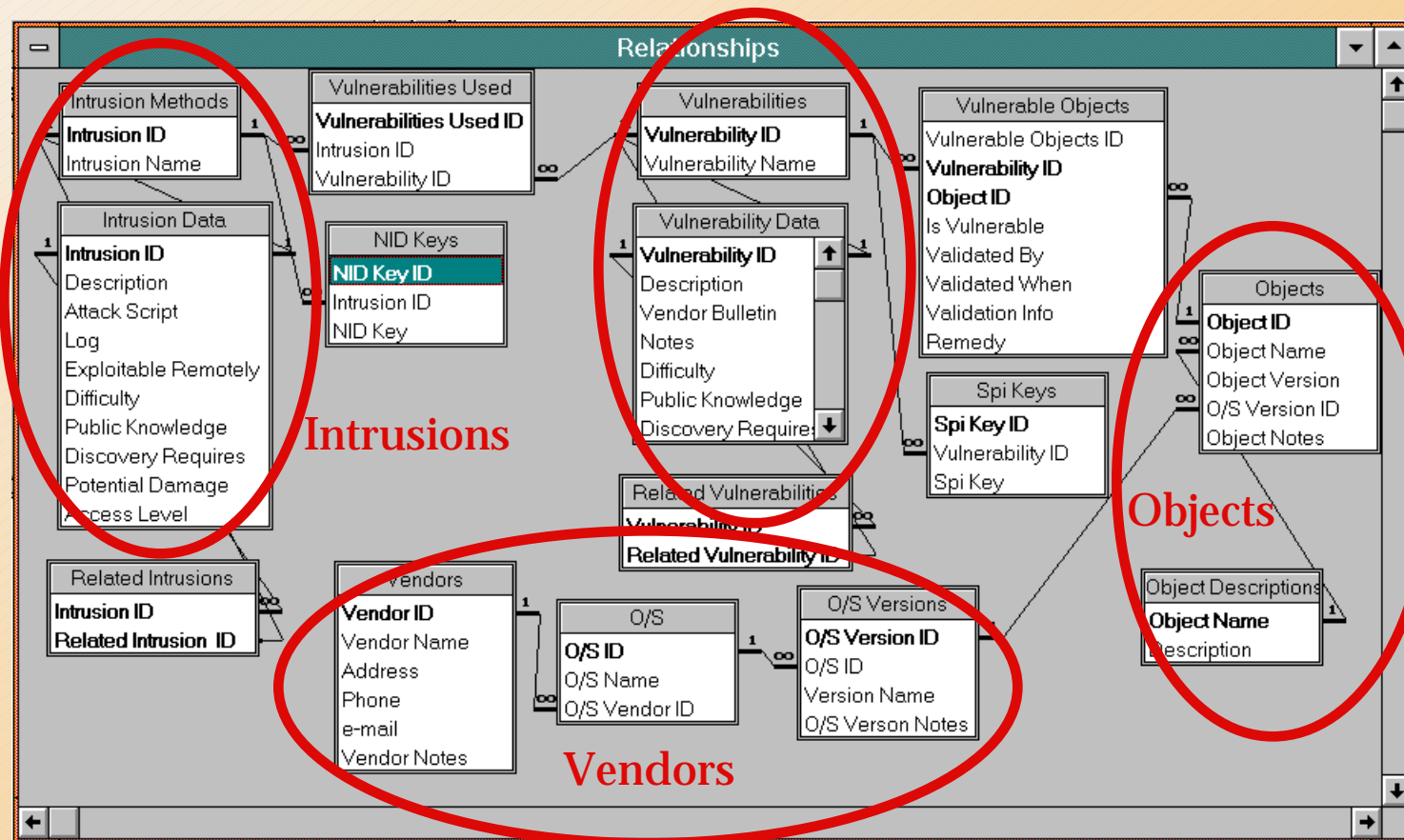
- **VAP is a project to identify and catalog computer system vulnerabilities in a framework that can be used both for analysis of vulnerabilities and for incident response.**
- **VAP data structures are being coordinated with other response teams.**
- **VAP will be accessible to DOE security managers.**

The VAP Server Is In Place

- **The server is based on a Sun Sparc 5 workstation behind the CSTC firewall.**
- **An Oracle server has been installed to hold the database.**
- **The database design is complete and implemented as an Access database.**
 - Access was used to speed the initial development.
- **The database is being populated.**

The Design Partitions the Information Into Four Distinct Parts

Vulnerabilities



First: Vendor Information

- The vendor information links the operating system versions and manufacturers.

The screenshot shows a web application window titled "Vendors". Inside, there is a form for "Vendor Name: SUN Microsystems, Inc". Below this, there are fields for "Address: 2550 Garcia Avenue MPK03-208 M", "Phone: (415) 688-9151", and "e-mail:". A "Vendor Notes" section contains the text: "FIRST: Mark Graff", "Phone: (415) 688-9151", and "STUlll: (415) 321-9259". Below the vendor information, there is a section for "O/S" with "O/S Name: SunOS". Underneath, there is a section for "O/S Versions" with "Version Name: 4.0.3" and an "O/S Ver. Notes:" field. At the bottom, there are three record navigation bars. The first two show "Record: 1 of", and the third shows "Record: 5 of 11".

Second: Objects

- The operating system objects are the files and structures that contain the flaw that allows the vulnerability to occur.

Objects

Object Name:

Object Version:

O/S Version

UNICOS	6.0
UNICOS	6.1
UNICOS	UNICOS
BSD	4.3
BSD	BDS
NeXTStep	1.0

Object Notes:

Record: 1 of 4

Object Description:

Record: 1 of 23

Third: Vulnerabilities

- The vulnerabilities show how to exploit the flaw in the operating system object.

The screenshot displays a web-based interface for managing vulnerabilities. The title bar reads "Vulnerabilities". Below the title bar are "New" and "Save" buttons. The form contains the following fields:

- Vulnerability Name:** Sendmail direct deliver to file
- Access:** A dropdown menu with options: All, Sensitive, Cray.
- Vendor Restricted:** An unchecked checkbox.
- Description:** This vulnerability allows a hacker to use sendmail to login to another user's account without password. A hacker can append his username to the victim's .rhost file by sending an electronic mail message directly to
- Vendor Bulletin:** SUN bug#1028173
- Vulnerable Obj Notes:** Recent versions of UNIX systems other than SunOS contains a sendmail fix. CIAC encourages you to consult with your vendor about this problem.
- Difficulty:** A dropdown menu with options: N/A, Shell, Shell Script, C, Difficult C, Kernel.
- Public Knowledge:** A dropdown menu with options: N/A, Theoretical, Never Seen, Occasionally Seen, Common, Rampant.
- Discovery Requires:** A dropdown menu with options: More than distribute, Source Code, Advanced Distribut, Standard Distribut, Access to Protocol, Public Access.
- Change Log:** On March 14, 1996, this entry was made. GHK
- Vulnerable Objects:** A table with columns: Object, Version, O/S, Version.

Object	Version	O/S	Version
/usr/lib/sendmail	66	SunOS	5.3

At the bottom of the form is a "Delete Object" button. The footer of the interface shows "Record: 1 of 23".

Fourth: Intrusions

- The intrusions show how to exploit the vulnerabilities to gain unauthorized access.

An Intrusion

Intrusions [New] [Save] [Open Vulnerability]

Intrusion Name: Bugs in 4.3BSD UNIX **Access:** All
Sensitive
Cray

Exploitable Remotely: ☐

Description: Several bugs exist in the operating system. For details, obtain the files from the UC system at "ucbarpa.berkeley.edu".

Attack Script: Depends on particular bug.

Log: This information was obtained on June 12, 1991.

Difficulty: N/A
Shell

Public Knowledge: Occasionally Seen
Common

Discovery Requires: Advanced Distribution
Standard Distribution

Potential Damage: Damage depends on the particular bug.

Vulnerabilities Used:

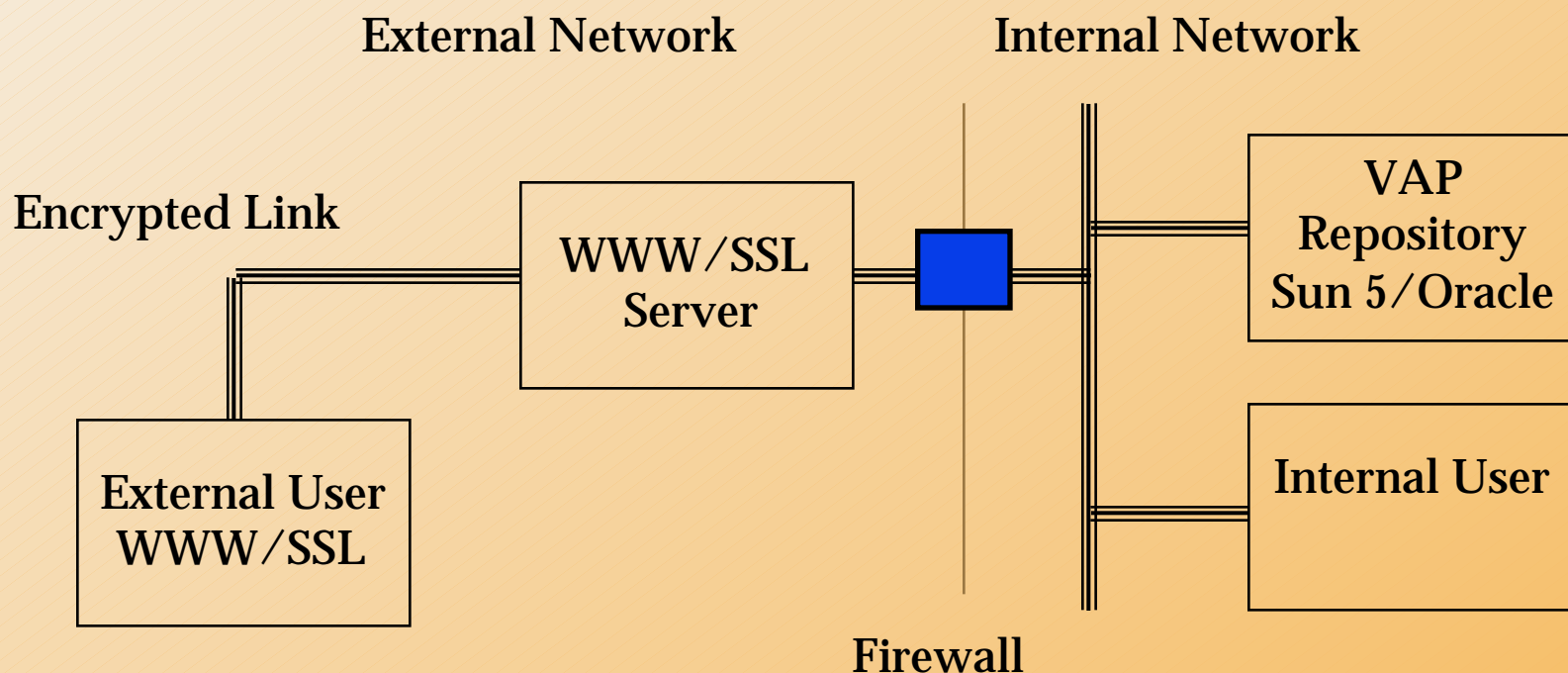
Bugs in 4.3BSD UNIX	11	35
---------------------	----	----

[Delete From Used]

Record: 1 of 23

The Repository Is Protected

- External users will use a web browser with an encrypted communication path.
- Access will be available to DOE security officers (*Real Soon Now*).



VAP Is A New Security Resource

- It will be available *real soon now* to DOE security managers.
- You will be able to search for vulnerabilities by name, system type, and other criteria.
- You will need world wide web access.
- You will need a browser that supports the secure socket layer (SSL) protocol.
- Access will be granted through your local DAA.